REMARKS/ARGUMENTS

These remarks are made in response to the Office Action of January 31, 2005 (Office Action). This response is filed after the 3-month shortened statutory period, and as such, a retroactive extension of time is herein requested. The Examiner is authorized to charge the appropriate extension fee to Deposit Account 50-0951.

In the Office Action, the Examiner has rejected claims 1-40 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,707,889 to Saylor, *et al.* (Saylor) in view of U.S. Patent No. 6,681,327 to Jardin (Jardin). Applicants filed a Reply on March 31, 2005 providing arguments to distinguish their claimed invention from the cited references.

In the Advisory Action of April 29, 2005 (Advisory Action) the Examiner indicated that the arguments of the Reply were not persuasive to the Examiner. According to the Advisory Action, the Application was not in a condition for allowance because Saylor discloses authenticating a user and Jardin disclosed a secure communication link between a client and a server. Combining Saylor with Jardin was believed to meet the limitations of the invention as previously claimed.

In response to the Advisory Action, Applicants have amended claims 1, 15, 21, and 35. Specifically, Claims 1, 15, 21, and 35 have been amended to clarify that the Voice Browser permits a user to audibly interact with Web content, as supported by page 3, lines 18-27 and throughout the specification. No new matter has been added.

Applicants emphasize that the Applicants' claimed and disclosed subject matter teaches a secure means for conveying VoiceXML content between a network device and a Voice Browser. Specifically, Applicants claim a solution for establishing a secure conduit or pipeline for conveying information ensuring that outside entities cannot obtain data as it is being transferred from point B (voice

browser) of the conduit to point C (network element) of the conduit. Known prior art and Examiner cited references fail to teach or suggest such a concept.

Saylor, for example, teaches a user authentication method. Once a user has been authenticated, Saylor allows the user to access user-specific information (Code keys associated with Web pages that an authenticated/registered user can access). Saylor provides no teachings pertaining to secure data conduits or transmission channels.

By a user authentication method, Applicants mean that Saylor teaches that a user (A) must authenticate itself to a server (B), which can include a voice browser, before being authorized to receive data (X) controlled by the server. This authentication is discussed in cited column 10, lines 17-40 and specifically at column 10, lines 35-37. Notably, data X can be obtained from a network element (C). Hence, data X is conveyed from C to B to A. Saylor fails to contemplate that the link a conduit C to B over which data X is conveyed is a secured and/or encrypted data conduit, as explicitly claimed by the Applicants.

The deficiencies of Saylor are not cured by Jardin. Jardin teaches a method and a system for speeding up secure client-server transactions by using a plurality of servers to assure that a server is available to transmit information whenever a client is ready to receive the information. Jardin teaches establishing a secure connection between a client and a broker. Jardin makes no specific reference regarding voice browsers.

Consequently, neither Saylor nor Jardin explicitly, inherently, nor implicitly provide teachings for establishing a secure data conduit or transmission channel between a voice server/browser and a data server (Web server) that provides content to the voice server/browser.

As noted in the background (page 1, line 18 to page 2, line 18), SSL has been typically integrated directly with selected underlying application protocols. Further,

PAGE 17/20 * RCVD AT 5/31/2005 12:52:48 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:5616596313 * DURATION (mm-ss):06-00

SSL compliant **visual** Web Browsers existed at the time of the Applicants' invention. As noted between page 3, lines 16 and page 4, line 21 of the background, at the time of the Applicants' invention, SSL had not been integrated with Voice Browsers. Neither Saylor, Jardin, nor combinations thereof provide such teachings or suggestions to integrate SSL (or other secure data conveyance conduit) with Voice Browsers, as claimed by the Applicants herein.

In terms of establishing a secure channel of communication, Voice Browsers are very different from Web browsers, which the Applicants shall take a moment to elaborate upon. In a Web browser, a user logs onto their computer (computer A) and accesses a network element (computer B). The user can load public keys, certificates, and other shared secret data on computer A. The data conduit between computer A and B is secured for a transaction, such as a transaction when a Web browser changes from "http" to "https" to indicate that a secure data transmission channel exists. Sensitive information, such as a credit card number, can be conveyed over this secure data channel. Conventional teachings provide various mechanisms for establishing the secure data channel between A and B, when A is a computer having a visual Web browser being used to access data from Web site (network element) B.

When a voice browser is utilized, a caller calls from a telephone (point A) to an interactive voice response system (IVR) having voice browsing capabilities (point B). The voice browser (B) can convey information between a network element (C). In this scenario, the user A does not control or "own" the voice browser (B) which is used by numerous telephone users. That is, according to conventional teachings, the voice browser does not have shared secret information that can be used to establish a secure data conduit with a network element.

The teachings of Jardin rely on conventional teachings where a client and a server (endpoints of a communication) both retain shared secret information. This is

PAGE 18/20 * RCVD AT 5/31/2005 12:52:48 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:5616596313 * DURATION (mm-ss):06-00

very different than the Applicants' claimed solution where the endpoint (telephone interface) does not include and/or retain shared secret information. Jardin fails to teach or suggest that a real time voice communication (ending in a telephone interface) is to consist of a voice link between a telephone interface and a voice browser and a SECURE DATA LINK between the voice browser and a data source.

To illustrate the deficiencies of prior art by way of example, consider the following. Before the Applicants' claimed invention, a user (via a telephone interface) may provide credit card number to a requesting IVR (automated voice response system) that in turn provides the credit card information to a network element. An intruder could intercept the credit card information between points B (the IVR) and C (the network element) and acquire the user's credit card number.

That is, computer system infiltrators recognized that the network connection from an IVR was a "security soft spot" that could be exploited, meaning that data traffic between the IVR and network element could be intercepted to obtain credit card data and other valuable information. The Applicants recognized this problem, and provided a solution that resolved the problem by establishing a secure data conduit between the voice browser and network elements. It is difficult for computer system infiltrators to improperly obtain data from the secure data conduit.

Neither Saylor nor Jardin address the above scenario in any fashion, which is directly addressed by the Applicants' claims. For example, Saylor fails to teach that a secure conduit is to be used to convey data from one point to another. The "user authorization" method of Saylor fails to prevent a computer system infiltrator from intercepting data/traffic and does not address the same problem.

Similarly, Jardin, fails to teach/suggest that some communications consist of both voice and data streams. Jardin is only concerned with client to broker communications (specifically with preventing bottlenecks using multiple servers for communications). Jardin does not contemplate providing secure data channels for

PAGE 19/20 * RCVD AT 5/31/2005 12:52:48 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:5616596313 * DURATION (mm-ss):06-00

voice browsers (that interact with a user via voice streams and with a network element via data streams), which is claimed by the Applicants.

In light of the above, Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned (direct line 954-759-8937) if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: 31 May 2005

Gregory A. Nelson, Registration No. 30,577
Brian K. Buchheit, Registration No. 52,667
AKERMAN SENTERFITT
Customer No. 40987
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000

PAGE 20/20 * RCVD AT 5/31/2005 12:52:48 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:5616596313 * DURATION (mm-ss):06-00